REMARKS

Overview of the Office Action

Claims 10 and 12 have been objected to for various informalities.

Claims 10 and 12 have been rejected under 35 U.S.C. §101 on the ground that the claimed invention is not tied to a particular machine.

Claims 2-4, 6-8, and 10-12 have been rejected under 35 U.S.C. §103(a) as unpatentable over U.S. Patent No. 6,505,215 ("Kruglikov") in view of U.S. Patent No. 6,824,064 ("Guthery"), and further in view of U.S. Patent No. 6,779,002 ("Mwaura"),.

Status of the claims

Claims 10 and 12 have been amended.

Claims 1, 5, and 9 have been previously canceled.

Claims 2-4, 6-8, and 10-12 remain pending.

Objection to the claims

Claims 10 and 12 have been objected to because the phrase "concluding or not" is interpreted as a step that does not have to be executed.

Claims 10 and 12 have been amended to remove the phrase "or not", thereby requiring that the step of "concluding by the application, whether a synchronization of the first and second databases is needed" must be executed.

Applicants submit that this objection has been overcome.

Rejection of claims 10 and 12 under 35 USC §101

The Office Action states that claims 10 and 12 have been rejected because the claimed invention is not tied to a particular machine. Applicants disagree.

Both claims 10 and 12 recite "a computer-implemented method". Clearly, claims 10 and 12 recite a method which is executed on and by a computer. Thus, the methods of claims 10 and 12 are, in fact, tied to a computer. Claims 10 and 12, moreover, recite and are tied to first and second data processing systems and a security token coupled to the first data processing system.

Applicants submit that this rejection should accordingly be withdrawn.

Rejection of claims 2-4, 6-8, and 10-12 under 35 USC §103(a)

The Office Action states that the combination of Kruglikov, Guthery, and Mwaura teaches all of Applicants' recited elements. Applicants disagree.

Independent claim 10 recites a computer-implemented method for synchronizing, through a network, a first database that is stored in a mobile first data processing system or in a security token coupled for communication with the mobile first data processing system, and a second database stored in a second data processing system. The recited method includes the steps of loading an application into the security token coupled to the mobile first data processing system, the application being operable to request that the mobile first data processing system start a synchronization process of the first database with the second database according to a synchronization policy; executing the loaded application in the security token; receiving, by the application, messages or events that occur in the mobile first data processing system or in the network; in response to the messages or events received and in accordance with the synchronization policy, concluding by the application whether a synchronization of the first and

second databases is needed and, if a synchronization is needed, transmitting, by the application, a command to the mobile first data processing system that informs the mobile first data processing system that a new synchronization is requested, the command providing the mobile first data processing system with information about synchronization parameters for use in synchronizing content of the first and second databases; and initiating, by the mobile first data processing system, the synchronization process of the first and second databases in response to receiving the command.

Kruglikov, Guthery, and Mwaura, whether taken alone or in combination, fail to teach or suggest a computer-implemented method for synchronizing, through a network, a first database that is stored in a mobile first data processing system or in a security token coupled for communication with the mobile first data processing system, and a second database stored in a second data processing system, where the method includes, "loading an application into the security token coupled to the mobile first data processing system, the application being operable to request that the mobile first data processing system start a synchronization process of the first database with the second database according to a synchronization policy", "receiving, by the application, messages or events that occur in the mobile first data processing system or in the network", and "in response to the messages or events received and in accordance with the synchronization policy, concluding by the application, whether a synchronization of the first and second databases is needed, and if a synchronization is needed, transmitting, by the application, a command to the mobile first data processing system that informs the mobile first data processing system that a new synchronization is requested, said command providing the mobile first data processing system with information about synchronization parameters for use in synchronizing content of the first and second databases", as recited in Applicants' claim 10.

Applicants' recited invention is concerned with the synchronization of a database contained in mobile equipment such as a mobile phone (i.e. the mobile first data processing system) with a database contained in a network operator server (i.e. the second data processing system).

The problem addressed by the recited invention is the need and ability to start the synchronization process according to a policy defined by a network operator in a context where the operator does not have the opportunity or access to implement a new application in the mobile equipment or to configure an already existing synchronization application that may be implemented in the mobile equipment.

There exist many types and varieties of mobile equipment, including mobile phones. The applications that can be executed by the mobile equipment can only be implemented and configured by the specific mobile equipment manufacturer. Each of the many mobile equipment manufacturers independently designs and constructs its mobile equipment for use by at least one of many different operators/networks that each typically employ different and distinct applications and functionality. Thus, such mobile equipment may be designed for use in different networks operated by different operators. The mobile equipment manufacturers are typically reluctant to install on their devices applications designed to work with only one specific network operator, as this would oblige the various mobile equipment manufacturers to design each mobile device for a specific network operator, which is inefficient and costly and, therefore, not a goal of the mobile equipment manufacturers.

Applicants' recited invention solves the above-described problem by loading a typically operator or network-supplied application into a security token, such as a SIM card, that is coupled to a mobile device/equipment, where the application is operable to request that the

mobile equipment start a synchronization process between a database stored in the mobile equipment and a database stored in a remote network operator server in accordance with a specific operator synchronization policy. The loaded application is executed in the security token, and receives messages or events that occur in the mobile equipment or in the network. In response to such messages or events that the loaded application receives, and in accordance with the synchronization policy, the loaded application determines whether a synchronization of the two databases is needed. If the loaded application determines that a synchronization is needed, then the loaded application transmits a command to the mobile equipment that informs the mobile equipment that a new synchronization is requested. Then, in response to the command, the mobile equipment initiates a synchronization of the two databases.

Using Applicants' recited method, the synchronization policy and parameters, which are specific to a particular network operator, are implemented in the security token that is coupled to the mobile equipment. Thus, the program to process the synchronization can be implemented in the mobile equipment, and that synchronization processing program can be the same for every network operator. Accordingly, Applicants' recited invention makes it possible to have mobile equipment, which is the same for every network operator, nevertheless apply a specific network operator-designed synchronization policy.

Kruglikov discloses a method and system for synchronizing two different computer systems (e.g., a personal computer system and a portable computer system) supporting multiple synchronization techniques (see col. 1, lines 39-41 of Kruglikov). Kruglikov teaches that the portable computer system is loaded with multiple synchronization transport modules (i.e., profiles). An application on the portable computer system of Kruglikov is executed, causing the application to automatically recognize the multiple synchronization transport modules. The

portable computer system receives from the remote system a selection identifying one of the multiple stored synchronization transport modules, and the portable computer system of Kruglikov then synchronizes with the other computer system using that selected synchronization transport module (see Abstract of Kruglikov).

The Examiner concedes that Kruglikov fails to teach or suggest a first data processing system that includes a security token, and that an application is loaded on the security token.

Consequently, Kruglikov also necessarily fails to teach or suggest that the application loaded on the security token requests that the mobile first data processing system start a synchronization process of the first database with the second database according to a synchronization policy (i.e., that the security token instructs the handset to perform a synchronization step), as recited in Applicants' claim 10. Instead, Kruglikov teaches that it is a user that launches the synchronization of his portable computer with his desktop personal computer (see col. 6, line 61 to col. 7, line 10 of Kruglikov).

The Examiner cites the Abstract, lines 1-7; col. 2, lines 1-14 and lines 51-57; col. 4, lines 25-29; and col. 7, lines 33-35 of Guthery as allegedly teaching a security token coupled for communication with the mobile first data processing system, and that an application is loaded into the security token.

Guthery discloses a system and method for moving the administration of simultaneous communication with multiple applications on a smart card onto the smart card itself. The smart card of Guthery includes memory that is logically partitioned into a plurality of memory blocks. A control program allocates one or more of the memory blocks of Guthery to one of the applications based on a declaration from the application of its memory needs, and schedules the applications for execution. Only those applications on the smart card of Guthery whose memory

needs have been satisfied are scheduled. The control program of Guthery receives a permission request packet from a host, addressed to an application, and passes the permission request packet to the application. When the control program of Guthery receives a permission packet from the addressed application after the addressed application has had its declared memory needs satisfied, the control program sends the permission packet to the host. A virtual machine is used to execute one or more of the applications of Guthery (see Abstract and col. 3, lines 41-48 of Guthery).

Guthery fails to teach or suggest that any of the applications loaded on the smart card are capable of, or intended for, requesting a mobile first data processing system initiate a synchronization process between a first database and a second database (see col. 3, lines 40-57).

In fact, Guthery mentions nothing regarding databases or synchronization. In stark contrast to Applicants' recited invention, the system of Guthery deals with the swapping of data pages between the smart card's memory and the host device. Further, even in this case, it is the host that commands that the swapping take place, not an application on the smart (see col. 4, lines 53-62 of Guthery).

The only updating taught by Guthery is when new applications are loaded onto the smart card by a loader application; the loader application then updates the directory of the applications (see col. 7, lines 33-35 of Guthery). Clearly, the updating of a directory of applications cannot in any way be construed as analogous to synchronization of databases.

Therefore, although Guthery teaches the use of a smart card, Guthery clearly fails to teach or suggest "loading an application into the security token coupled to the mobile first data processing system, the application being operable to request that the mobile first data processing system start a synchronization process of the first database with the second database according to

a synchronization policy", as recited in Applicants' claim 10.

The Examiner additionally cites the Abstract, lines 1-29; and col. 6, lines 20-38 of Mwaura as teaching receiving a message by an application and concluding if synchronization is needed by checking if the message is relevant and, if so, taking a synchronization action.

Mwaura discloses a computer software framework and method for synchronizing data across multiple databases. The method for synchronizing data includes instantiating a first data synchronization service object and a second data synchronization object. The first data synchronization service object is connected to a first datastore, and the second data synchronization service object is connected to a second datastore. A data synchronization message containing relevant information is sent from the first data synchronization service object to an outbox queue on the first datastore. The data synchronization message is propagated from the outbox queue on the first datastore to an inbox queue on the second datastore. The data synchronization message is received from the inbox queue on the second datastore to the second data synchronization object, and the relevant information is persisted in the second datastore (see Abstract of Mwaura).

In other words, Mwaura is concerned with the synchronization of common data between applications with unique schemas on different databases of different business units of the same company (see col. 1, lines 16-33 of Mwaura). According to Mwaura, various computing systems of an enterprise may synchronize their common data without requiring them to share databases or have similar database schemas. The framework described by Mwaura does not in any way involve synchronizing a database that is on a mobile device with a database on another processing system.

Mwaura fails to teach or suggest anything whatsoever regarding security tokens or loading an application into a security token coupled to a mobile first data processing system, where the application is operable to request that the mobile first data processing system start a synchronization process of a first database with a second database according to a synchronization policy.

Furthermore, the Examiner's proffered combination of Kruglikov, Güthery, and Mwaura is improper because there is in fact absolutely no motivation, absent Applicants' own teachings, to combine these references in the manner suggested by the Examiner. Applicants' recited invention is directed to a situation in which a user of a mobile device must synchronize a first database on the mobile device with a second, remote database to which the user has no access. The application that facilitates this synchronization of the first and second databases is stored and executed on a security token that is supplied and controlled by the entity that also controls the second database. In practice, Applicants' security token may, by way of example, include a subscription related application that is provided by a service provider or network operator.

In contrast, Kruglikov teaches the synchronizing of two different computers that are both owned by, or accessible to, a single user. Thus, according to the teachings of Kruglikov, new synchronization applications can be easily implemented and configured on the portable computer. Likewise, Mwaura teaches the synchronizing of different databases of different business units of the same company -- i.e. under the same control -- and does not involve synchronizing a database on a mobile device.

In contrast, the problem solved by Applicants' recited invention, which is to synchronize two databases that are not both accessible to or controlled by the user, is of no concern or is simply not a consideration of Kruglikov or Mwaura.

In view of the above, there is no absolutely no reason or motivation in the cited art to use a security token, which includes an application that is under a separate entity's control, to synchronize the two computers of Kruglikov (or the two databases of Mwaura) based on instructions received from such separate entity. When a user of the computers of Kruglikov wishes to synchronize the two computers, he or she simply proceeds and does so at his or her convenience. Likewise, when one business unit of Mwaura wishes to synchronize its database with a database of another business unit, the synchronization is simply executed.

Moreover, as pointed out above, Guthery fails to teach or suggest that an application on the SIM card is operable to request a mobile first data processing system to start a synchronization process of a first database with a second database according to a synchronization policy, or that the proactive command is a command to the mobile first data processing system that informs the mobile first data processing system that a new synchronization is requested, and that the command provides the mobile first data processing system with information about synchronization parameters for use in synchronizing content of the first and second databases, as recited in Applicants' claim 10.

Consequently, even if one skilled in the art were to artificially combine the teachings of Kruglikov, Guthery, and Mwaura, the resulting system would still not result in Applicants' recited invention.

Instead, the resulting artificial combination would at most simply provide a method of synchronizing two computers or databases, both accessible to or controlled or owned by the same user, where a portable one of the computers includes a SIM card that is capable of executing some command.

Combining these references does not result in a portable computer that includes a SIM card which includes an application that is under a separate entity's control to synchronize a first database that is owned by or accessible to the user with a second database that is not owned by, accessible to, or controlled by the user.

Independent claim 12 recites limitations similar to those of claim 10 and is, therefore, deemed to be patentably distinct over Kruglikov, Guthery, and Mwaura for at least those reasons discussed above with respect to independent claim 10.

In view of the foregoing, it is clear that Kruglikov, Guthery, and Mwaura, whether taken alone or in combination, fail to teach or suggest the subject matter now recited in independent claims 10 and 12. Accordingly, claims 10 and 12 are deemed to be patentable over Kruglikov, Guthery, and Mwaura under 35 U.S.C. §103(a).

Claims 2-4, 6-8, and 11, which depend from independent claim 10, incorporate all of the limitations of independent claim 10 and are, therefore, deemed to be patentably distinct over Kruglikov, Guthery, and Mwaura for at least those reasons discussed above with respect to independent claim 10.

Conclusion

In view of the foregoing, reconsideration, and withdrawal of all rejections, and allowance of all pending claims, are respectfully solicited.

Should the Examiner have any comments, questions, suggestions, or objections, the Examiner is respectfully requested to telephone the undersigned.

Respectfully submitted,
COHEN PONTANI LIEBERMAN & PAVANE LLP

By /Lance J. Lieberman/
Lance J. Lieberman
Reg. No. 28,437
551 Fifth Avenue, Suite 1210
New York, New York 10176
(212) 687-2770

Dated: May 26, 2009